Principles and Foundations for Fractionated Networked Cyber-Physical Systems

Quarterly Report

Mark-Oliver Stehr **Pat Lincoln**

Date of Preparation: 06/14/2010
Period covered: 04/01/2010 - 06/15/2010

Project Abstract A new generation of mission-critical systems is emerging that employs distributed, dynamically reconfigurable open architectures. These systems may include a variety of devices that sense and affect their environment and the configuration of the system itself. We call such systems *Networked Cyber-Physical Systems* (NCPS). NCPS can provide complex, situation-aware, and often critical services in applications such as distributed sensing and surveillance, crisis response, self-assembling structures or systems, networked satellite and unmanned vehicle missions, or distributed critical infrastructure monitoring and control. NCPS are of special interest to the Navy in view of the increasing need for coordination of a wide spectrum of maritime sensing and information gathering technologies, ranging from smart mobile buoys to autonomous underwater vehicles and their integration into a global network with maritime, space, and ground domains.

NCPS must be reactive and maintain an overall situation, location, and time awareness that emerges from the exchange of knowledge. They must achieve system goals through local, asynchronous actions, using (distributed) control loops through which the environment provides essential feedback. They must deal with uncertainty and partial knowledge, and be capable of a wide spectrum of operations between autonomy and cooperation to adapt to resource constraints and disruptions in communication. General principles and tools are needed for building robust, effective NCPS. A key observation is that the current level of abstraction at which software and systems are designed is a barrier to innovation at the hardware and networking level and at the same time is not suitable to enable rapid design/deployment or distributed control of large-scale distributed software

systems and in particular the flexible, dynamically reconfigurable, mission-critical NCPS of the future.

We propose to explore a new paradigm for design of high-assurance NCPS based on the notion of software fractionation with declarative distributed control and optimization aiming at the effective use of resources. The idea of software fractionation is inspired by and complementary to hardware fractionation, which has been proposed for mission-critical space systems. Fractionation has the potential of leading to software that is more robust, leveraging both diversity and redundancy. It raises the level of abstraction at which control and optimization techniques are applied.

1 Project Activities

In the first two months of the project we have layed out the general scope of the project and developed a specific research plan for the first phase. Starting with some motivation, we briefly summarize our approach, the potential impact, the research goals, and our progress up to this point.

1.1 Motivation and Approach

We observe that today and in the future military success will critically depend on NCPS, but the state of the art is discouraging. Principles and foundations to design and understand NCPS are missing and software for NCPS is designed using inadequate conventional paradigms. Conventional software is inflexible, not adaptive to resources, and requires many assumptions on its environment, which make it fragile and vulnerable. Furthermore, due to the lack of a common foundation, software is redeveloped at high cost in many variants for different settings.

In this project we adopt a view of cyber-physical systems that goes beyond the conventional definition of a hardware/software system that is interacting with the physical world. Our goal is to explore a new notion of software that behaves itself closer to a physical or biological system. In other words, we aim to address the fundamental problem by reducing the sharp boundary between physics and computation. Our rationale is that current models of distributed computing are too abstract by not taking into account fundamental physical limitations and hence are not efficiently implementable or scalable. Once limitations can be explicitly represented, they can be over-

come to some degree, which can be quantified, e.g. probabilistically. Like in biological systems, diversification, redundancy, and randomization should be utilized to overcome physical limitations whenever possible. In particular, distribution is a source of redundancy and diversification that can be turned from an obstacle into an advantage.

In our approach, software is fractionated by design even beyond the distributed nature of underlying system, with distributed knowledge sharing as the underlying model. Computation and communication is not rigid but guided by the physical resources, e.g. in an opportunistic fashion. Our vision that that fractionated software operates as an inherently open system in a highly redundant and diversified way avoiding single points of responsibilities and failure. Being resource-aware, fractionated software operates in the entire spectrum between autonomy to cooperation. Our distributed computing model is based on distributed knowledge sharing, and makes very few assumptions but restricts the shape of fractionated software so that it can run on a wide range of platforms. In particular it does not assume strong primitives that are powerful but not implementable in a scalable way.

1.2 Potential Impact

Although partly beyond the scope of this project we expect possible applications and potential impact of our work in many areas. In mission-critical NCPS, fractionated software may lead to improved robustness, reliability, and flexibility. It can take into account the heterogeneous nature of the network and can better utilize the resources. It should enable rapid development and deployment at lower cost, and finally support new technologies or challenging environments that are beyond the reach of conventional software. Potential applications beyond NCPS include scalable computing with heterogeneous, parallel architectures (from many-core to clusters, e.g. grid/cloud), computing with highly unreliable components (e.g. processors, storage, networking, sensors), and mobile/social computing with intermittent connectivity (e.g. PDAs with or without networking infrastructure).

1.3 Goals and Progress

Our specific research goals for Phase 1 are to develop theoretical foundations of fractionated software, to study relationships with other distributed computing models, and design a fractionated software framework that will allow

us to conduct various experiments.

To benefit from synergies with other projects at SRI, we are holding a multi-disciplinary research seminar around the topic of NCPS. We have also started to develop the theoretical foundations of fractionated software based on the distributed knowledge sharing model. For instance, key principles behind the fractionated model are strong locality of computations without the possibility of distributed arbitration and the partial anonymity/indistinguishability of network nodes to avoid a rigid binding of computation to physical locations. First steps in the formalization of these principles have been made and are promising. In parallel, we are in the process of identifying typical patterns of fractionated software. One common pattern, namely the distributed execution of multiple tasks in a self-organizing fashion, i.e. without a global coordinator, has been successfully modeled in what we call a Stochastic Task Execution Model (STEM) and analyzed using Monte Carlo techniques.

Our plans for the next reporting period is to finalize the formal definition of fractionated software, establish some key properties, and conduct further experiments, e.g. with refined models and other typical distributed software patterns.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
06/14/2010	Quarterly Report	04/01/2010 - 06/15/2010

4. TITLE AND SUBTITLE
Principles and Foundations for Fractionated Networked Cyber-Physical Systems

5a. CONTRACT NUMBER

5b. GRANT NUMBER
N00014-10-1-0365

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Dr. Mark-Oliver Stehr
Dr. Patrick Lincoln

5d. PROJECT NUMBER
I0PR04183-00

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025-3493

8. PERFORMING ORGANIZATION REPORT NUMBER
PI9458 Qrt 1

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of Naval Research
875 North Randolph Street
Arlington, VA 22203-1995

10. SPONSOR/MONITOR'S ACRONYM(S)
ONR

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for Public Release, Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
We propose to explore a new paradigm for design of high-assurance Networked Cyber-Physical Systems based on the notion of software fractionation with distributed control and optimization aiming at the effective use of resources. The idea of software fractionation is inspired by and complementary to hardware fractionation, which has been proposed for mission-critical space systems. In our approach, software is fractionated by design even beyond the distributed nature of underlying system, with distributed knowledge sharing as the underlying model. Computation and communication is not rigid but guided by the physical resources, e.g. in an opportunistic fashion. Fractionation has the potential of leading to software that is more robust, leveraging both diversity and redundancy. It raises the level of abstraction at which control and optimization techniques are applied. In the first two months of the project we have layed out the general scope of the project and developed a specific research plan for the first phase. First steps in the formalization of these principles have been made. In parallel, we are in the process of identifying typical patterns of fractionated software.

15. SUBJECT TERMS
Fractionated Software, Distributed Computing, Networking, Cyber-Physcial Systems

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Kathryn Tracy
u	u	u	uu		19b. TELEPHONE NUMBER *(Include area code)* 650-859-3435